

Robust Image Encryption Using Discrete Fractional Fourier Transform with Eigen Vector Decomposition Algorithm

Deepak Sharma^{*1}, Rajiv Saxena², Ashutosh Rajput³

^{*1,2}Department of Electronics and Communication, Jaypee University of Engineering and Technology, Guna (M.P.) Postcode - 473226, India

³Department of Electronics and Communication, Modern Institute of Technology and Research Centre, Alwar, Postcode - 301028, India

^{*}deepakforu23@rediffmail.com; ²rajiv.saxena@juet.ac.in

Abstract

Numerous methods have been recently proposed in the literature for the encryption of 2-D information using optical systems based on the Fractional Fourier Transform. Encryption is one of the well known techniques to provide security in transmission of multimedia contents over the internet and wireless networks. There is a vast use of image in all areas so its security is of great concern nowadays. Discrete Fractional Fourier Transform (DFRFT) generalization of the Discrete Fourier transform (DFT) with an additional parameter is incorporated in image encryption to achieve a more robust encryption system. To focus on security aspect, in this paper a novel method of image encryption has been proposed based on discrete Fractional Fourier Transform (DFRFT), using exponential random phase mask. Encryption with this technique makes it almost impossible to retrieve an image without using both the correct keys. The technique has been implemented experimentally and parameters like security, sensitivity and mean square error (MSE) are discussed.

Keywords

Fourier Transform (FT); Discrete Fourier Transform (DFT); Fractional Fourier Transform (FRFT); Discrete Fractional Fourier Transform (DFRFT).

Introduction

Fourier transform was first introduced by the French scientist Jean Baptiste Joseph Fourier, in 1807 [17]. After that FT was applied in all the fields of science and engineering. Fractional Fourier Transform was introduced as the generalization of Fourier Transform, thus creating a scope of improvement where Fourier transform was applied along with time varying signal analysis. It has been applied to various areas like signal processing, optics and quantum mechanics. The discrete fractional Fourier transform (DFRFT) is a generalization of the DFT with additional free

parameters defined by Pei and Ozaktas. Pei and Yeh defined the DFRFT based on the eigen decomposition of the DFT matrix, and a DFRFT with one fractional parameter was defined by taking fractional eigen value powers of an eigen decomposition of the DFT matrix. The DFT eigenvectors used are Hermit Gaussian type. These eigenvectors are computed from a DFT commuting matrix proposed by B. W. Dickinson and K. Steiglitz. Pei et al. first proposed the eigen decomposition- based definition of the DFRFT, and then Candan et al. consolidated this definition .

In recent years, there has been great concern over information security. Various optical encryption methods have been proposed by researchers in the past two decades. More robust encryption schemes are always required to protect data. Which can be fulfilled by proposing a more robust transform and applying this transform in a model to achieve more unauthorized user protected scheme for encryption.

In proposed encryption scheme, Discrete FRFT was utilized with the double random phase encoding to enhance its data security for input grayscale image. An image was encrypted using DFRFT with double random phase matrix and an image decrypted by using same key utilized for encryption. In proposed scheme, two keys are utilized to encrypt an image which enhances the robustness and security of the system. The security key is highly sensitivity to deviation of correct keys and it has also been investigated in simulated results.

The outline of this paper is as follows: In section II we discuss the FRFT and DFRFT briefly. In section III we discuss the proposed DFRFT based image encryption model with double random phase matrix. In section IV the security, sensitivity and MSE of for an image have

been investigated. In section V the results are summarized.

Preliminaries

Fourier transform is the rotation of a signal by an angle of $\pi/2$ in time frequency plane. The fractional Fourier transform removes the constraint of Fourier transform and allows rotation of angle ' α ' where it is a multiple of $\pi/2$. The FRFT of signal $x(t)$ of order ' p ' can be represented as,

$$X_p(u) = \int_{-\infty}^{\infty} x(t) K_p(u, t) dt. \quad (1)$$

There is a relation between the angle of rotation ' α ' and order given as $\alpha = p\pi/2$. The kernel K_p is defined as,

$$K_p(u, t) = \begin{cases} \sqrt{\frac{1-j \cot \alpha}{2\pi}} \exp(j \frac{t^2+u^2}{2} \cot \alpha - jut \csc \alpha) & \alpha \neq n\pi \\ \delta(t-u) & \alpha = 2n\pi \\ \delta(t+u) & \alpha = (2n \pm \pi) \end{cases} \quad (2)$$

As the development goes on in the field of digital signal processing, there is a need for discrete fractional Fourier transform for all applications using fractional Fourier transform because all the signals processed in discrete form. DFRFT is the generalization of the discrete Fourier transform (DFT) with an additional parameter. Some basic properties of DFRFT are

- 1) Unitary
- 2) Additive
- 3) Reduction to DFT when order is equal to unity.

The $M \times M$ DFT matrix can be expressed as,

$$X = \frac{1}{\sqrt{M}} e^{-j \frac{2\pi}{M} km} \text{ for } K \geq 0, m \leq M-1 \quad (3)$$

Matrix X has only four distinct Eigen values 1, -1, j and $-j$. Now a $M \times M$ matrix Z is defined whose entries are

$$\begin{aligned} Z_{m,m} &= 2 \cos\left(\frac{2\pi}{M} n\right), \quad 0 \leq n \leq M-1 \\ Z_{m,m+1} &= Z_{m+1,m} = 1, \quad 0 \leq n \leq M-2 \\ Z_{M-1,0} &= Z_{0,M-1} = 1 \end{aligned} \quad (4)$$

Now as $ZX=XZ$, i.e. they commute with each other, and have same value of eigen vector but different eigen values. Now $M \times M$ DFRFT matrix can be defined as,

$$X^\alpha = V D^\alpha V^T$$

$$= \begin{cases} \sum_{k=0}^{M-1} e^{-j \frac{\pi}{2} k \alpha} v_k v_k^T & \text{for } M = \text{odd} \\ \sum_{k=0}^{M-2} e^{-j \frac{\pi}{2} k \alpha} v_k v_k^T + e^{-j \frac{\pi}{2} M \alpha} v_M v_M^T & \text{for } M = \text{even} \end{cases} \quad (5)$$

Here D is the diagonal matrix and T is the transpose. The matrix V is defined as,

$$\begin{aligned} V &= [v_0, v_1, \dots, v_{M-2}, v_{M-1}] \quad \text{for } M = \text{odd} \\ V &= [v_0, v_1, \dots, v_{M-2}, v_M] \quad \text{for } M = \text{even} \end{aligned} \quad (6)$$

This is known as eigen decomposition form of DFRFT.

Proposed Model for Encryption and Decryption

Encryption

Encryption, a very ancient technique, is a process in which information is secured with the help of a key to protect it from an unauthorized person. The information which has to be encrypted can be in the form of a text or an image etc. Encrypted information should not give any idea about the original information. In the proposed method, image encryption of gray scale image is done using double random discrete fractional Fourier transform. In Gray scale image, the value of each pixel carries only intensity information ranging from 0 to 255. They also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest.

In double random matrix DFRFT method, the input image is multiplied with the first exponential random matrix S after that the DFRFT of order ' α ' is applied then, the resulting matrix is multiplied by the second exponential random matrix C and again DFRFT of order ' β ' is applied to get the encrypted image. The random matrices at encryption and decryption should be orthogonal to each other.

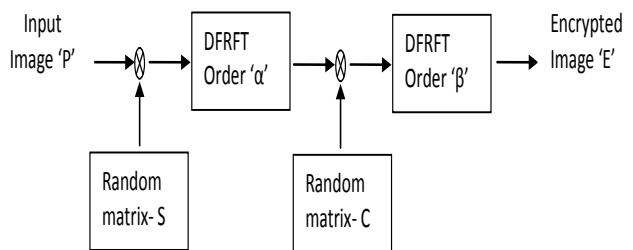


FIG. 1 IMAGE ENCRYPTION MODEL

Exponential random matrix S and C should be independent of each other. The value of S and C are. $S = e^{j\varphi n}$, $C = e^{j\beta m}$

Now let us understand the mathematics of the proposed encryption process.

$$W' = P \otimes e^{j\varphi n} \quad (7)$$

where P is input image matrix multiplied by S , the random matrix

$$W'' = X^\alpha (P \otimes e^{j\varphi n}) \quad (8)$$

DFRFT of order α is applied.

$$W''' = (X^\alpha (P \otimes e^{j\varphi n})) \times e^{j\beta m} \quad (9)$$

Then it is multiplied by random matrix C .

$$E = X^\beta ((X^\alpha (P \otimes e^{j\varphi n})) \times e^{j\beta m}) \quad (10)$$

Then DFRFT of order β is applied to get the encrypted Image E .

Decryption Model

It is the process of retrieving the original information from the encrypted form as well as reverse process of the encryption part. Input is an encrypted image in decryption model. Input image 'E' is taken then DFRFT of order ' $-\beta$ ' is applied then to it, and random matrix C^* is multiplied which cancel out the effect of random matrix C as they both are orthogonal to each other. To the resulting matrix DFRFT of order ' $-\alpha$ ' is applied then multiplied by the random matrix S^* to get the decrypted image.

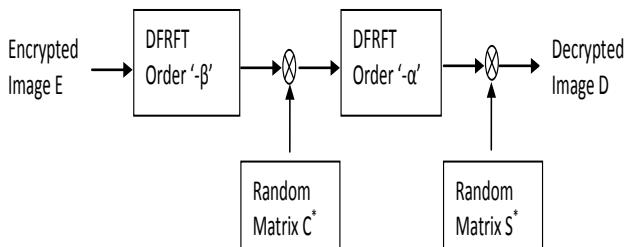


FIG. 2 IMAGE DECRYPTION MODEL

The Decryption model mathematically given as,

$$\begin{aligned} E' &= X^{-\beta}(E) \\ &= X^{-\beta}(X^\beta(X^\alpha(P \otimes e^{j\varphi n}) \otimes e^{j\beta m})) \end{aligned} \quad (11)$$

Then it is multiplied by the random matrix C^* as it will cancel out the effect of C as they are orthogonal.

$$E'' = (X^{-\beta}(X^\beta((X^\alpha(P \otimes e^{j\varphi n}) \otimes e^{j\beta m}))) \otimes e^{-j\beta m}) \quad (12)$$

Now, DFRFT of order $-\alpha$ is applied

$$E''' = X^{-\alpha}((X^{-\beta}(X^\beta((X^\alpha(P \otimes e^{j\varphi n}) \otimes e^{j\beta m}))) \otimes e^{-j\beta m})) \otimes e^{-j\varphi n} \quad (13)$$

Then random matrix S^* , is multiplied

$$D = (X^{-\alpha}((X^{-\beta}(X^\beta((X^\alpha(P \otimes e^{j\varphi n}) \otimes e^{j\beta m}))) \otimes e^{-j\beta m})) \otimes e^{-j\varphi n}) \otimes e^{-j\varphi n} \quad (14)$$

Where D is the decrypted image and after solving it

gives original image 'P' as output.

Salient Features

Security

Security is the main aim. The key here is formed, by the combination of the order of discrete fractional Fourier transform and the random phase matrix. In encryption model various possible combination provides formidable key sets, thus providing higher amount of security. This is also effective against brute force attack i.e. if all the set of key are known. In this case as the key set is large and the time taken is very large in brute force attack thus making it impractical to crack the correct key.

Sensitivity

The model of encryption and decryption should be highly sensitive with respect to the variation of correct key i.e. if the any key other than the correct key is used, it will not decrypt the correct input image. result with our simulation. It has been checked that our image is much sensitive to the deviation in the original key.

Complexity

If complexity of system increases it usually also improves the security of system. There is a tradeoff between the complexity and the security of a system required. It is also analyzed based on the property of the utilized discrete fractional Fourier transform (DFRFT) that the encryption scheme can be realized by the fast Fourier transform (FFT)-based algorithm. In proposed algorithm encryption and the decryption procedures are both realized by the matrix multiplications. For an image with a size of $A \times B$, the complexity of the encryption and the decryption is about equal to $A^2 B + B^2 A$ complex multiplications.

Results

In this paper, an image has successfully encrypted and decrypted using DFRFT with double random phase matrix. Simulation of the proposed method has been done on a grayscale image of Lena of dimension 300×300 . The image was encrypted for the selected orders $\alpha = 0.8$, $\beta = 1.2$ by using two exponential random matrices S and C which are independent to each other. As it can be seen that fig. 3 (a) is the original image and after encryption an encrypted image is obtained as shown in the fig 3(b). In decryption process we have to apply the order $a = -0.8$ and $\beta = -1.2$ to get the

correct decrypted image observed in the figure 3(c) and if the proper value of the order is not used then it will not give the correct result as observed in fig 3(d). Here the orders are $\alpha = 0.9$, $\beta = 1.1$. The image can be decrypted only by using the correct order.



FIG. 3(A) ORIGINAL IMAGE

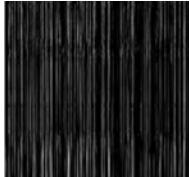


FIG. 3(B) ENCRYPTED IMAGE



FIG. 3(C) DECRYPTED IMAGE (CORRECT KEY)

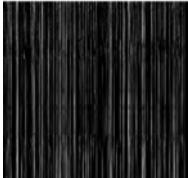


FIG. 3(D) DECRYPTED IMAGE (WRONG KEY)

FIG.3 IMAGE ENCRYPTION USING DOUBLE RANDOM MATRIX DFRFT METHOD (A) ORIGINAL IMAGE (B) ENCRYPTED IMAGE FOR A = 0.8, B = 1.2. (C) DECRYPTED IMAGE WITH CORRECT PARAMETER A = 0.8, B = -1.2 (D) DECRYPTED IMAGE WITH WRONG PARAMETER A=0.9,B=1.1.

As the result shows that encrypted image doesn't give any idea about the original image and image can be decrypted only by the use of correct key as shown in Fig. 3(c) and if correct, it is not used, original image cannot be retrieved as shown in fig. 3(b). Thus, the proposed method encrypts and decrypts image properly. Histogram of the image plots frequency of each pixel value, and summarizes the intensity of an image.

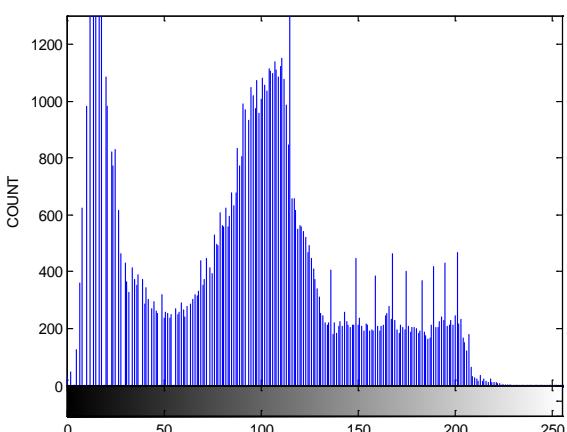


FIG. 4(A) HISTOGRAM OF ORIGINAL IMAGE

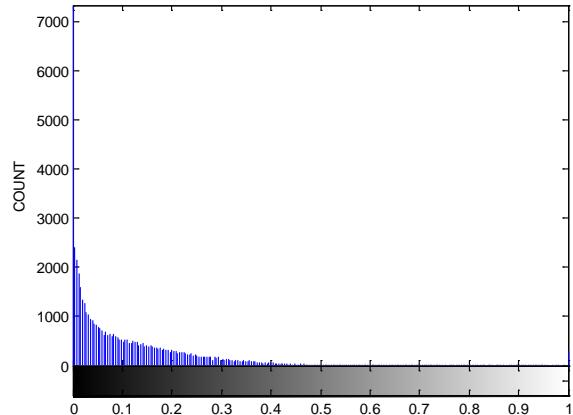


FIG. 4(B) HISTOGRAM OF AN ENCRYPTED IMAGE

FIG. 4 HISTOGRAM OF AN ORIGINAL AND ENCRYPTED IMAGE

In fig 4.(a) and 4.(b), the histogram of an original image and the encrypted image of Lena are shown. As it can be seen that the histogram of the encrypted image is completely different from that of original image so it does not give any idea to unauthorized person to carry on the attack.

MSE (mean square error) is calculated between the original image and decrypted image given by,

$$MSE = \frac{1}{MN} \sum_{m=1}^M \sum_{n=1}^N [\bar{P}(m,n) - P(m,n)]^2$$

Where M and N indicate the size of the image while $\bar{P}(m,n)$ and $P(m,n)$ indicate the original and decrypted image of pixel (m,n) respectively.

TABLE-1 MSE OF DIFFERENT IMAGES

IMAGE	MEAN SQUARE ERROR (MSE)		
	Min	Max	Avg
Lena	2.6754×10^{-13}	4.3435×10^{-13}	3.2457×10^{-13}
Camera man	3.4593×10^{-13}	5.7725×10^{-13}	4.3491×10^{-13}
Spine MRI	3.5514×10^{-13}	4.7220×10^{-13}	4.0645×10^{-13}

MSE of different images are calculated to check the consistency of the proposed technique. The size of images can be different and tested for various size of images with same scheme. The results are obtained over 201 iterations for each image to get the result as shown in the table-1. The proposed scheme is quite consistent with different images for encryption/decryption verified with the results shown in table-1.

In fig. 5 the sensitivity of key is shown, and image will be correctly decrypted only by the use of original key, if there is small deviation from the original key then it will show a sharp increase in the normalized MSE. Comparison between the sensitivity of FRFT and DFRFT is done. DFRFT is more sensitive to the

deviation in the correct key. So proposed scheme is highly sensitive with respect to their original key. Small deviation from original key provides large error and wrong detection of the image.

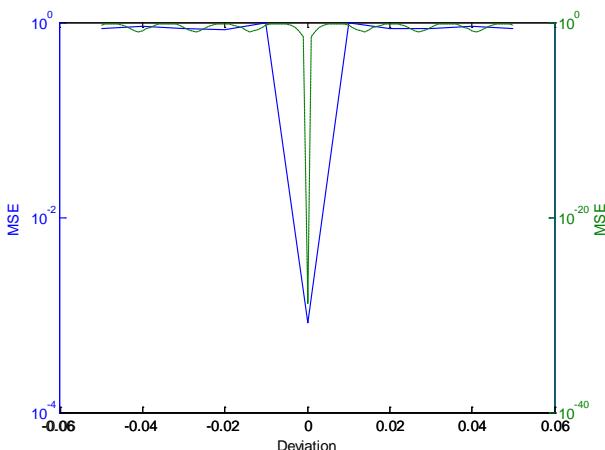


FIG.5 NORMALIZED MSE BETWEEN THE DECRYPTED IMAGE AND ORIGINAL IMAGE AS A FUNCTION OF DEVIATION IN THE FRACTIONAL ORDER USED FOR DECRYPTION FOR DFRFT AND FRFT

Conclusions

In this paper, a novel method has been proposed for image encryption using discrete fractional Fourier transform with double random matrix. The DFRFT used here is eigen vector decomposition type. The minimum MSE achieved here is 2.6754×10^{-13} for Lena image. The decryption is highly sensitive towards the original key as shown in fig. 5 compared to the FRFT based scheme. The system is more sensitive to the correct key if the key deviate by more than .01 value with their original key, MSE increases and original image cannot be decrypted. The complexity of the system increases with DFRFT comparatively using FRFT in the same system. The histogram also verifies our results that the encrypted image has almost uniform distribution of data so original image cannot be decoded successfully. The DFRFT based image encryption schemes is better and more sensitive but produces more complexity than FRFT based encryption scheme.

ACKNOWLEDGMENT

The authors thankfully acknowledge all the authorities of Jaypee University of Engineering & Technology, Guna (M.P.) - 473226, INDIA.

REFERENCES

B. Hennelly, Sheridan JT: Optical image encryption by

- random shifting in fractional Fourier domains. Opt. Lett. 28 (2003) :269–71.
- B. Javidi, A. Sergent, G. Zhang, and L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," Opt. Eng. 36, 1997:992-98.
 - B. M. Hennelly and J. T. Sheridan, "Image encryption based on the fractional Fourier transform," Proc. SPIE, vol. 5202, 2003: 76-87.
 - B. W. Dickinson and K. Steiglitz, "Eigenvectors and functions of the discrete Fourier transform," IEEE Trans. Acoust., Speech, Signal Process., vol. ASSP-30, Jan. 1982:25-31.
 - B. Zhu , Liu S, Ran Q: Optical image encryption based on multifractional Fourier transforms. Opt. Lett. 25 (2000): 1159–61.
 - C. Candan, M. A. Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," IEEE Trans. Signal Process., vol. 48, no. 5, May 2000:1329-37.
 - G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double random phase encoding in the fractional Fourier domain," Opt. Lett., vol. 25, no. 12, 2000: 887-89.
 - G. Unnikrishnan and K. Singh, "Double random fractional Fourier-domain encoding for optical security," Opt. Eng., vol. 39, 2000:2853-59.
 - G. Unnikrishnan and K. Singh, "Optical encryption using quadratic phase systems," Opt. Commun. 193, 2001:51-67.
 - H. Al-Qaheri, A. Mustafi, and S. Banerjee, "Digital watermarking using ant colony optimization in fractional Fourier domain," J. Inf. Hiding Multimedia Signal Process., vol. 1, no. 3, Jul. 2010:179-89.
 - H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, The Fractional Fourier Transform with Applications in Optics and Signal Processing. New York: Wiley, 2000.
 - L. B. Almeida, "The fractional Fourier transform and time-frequency representations," IEEE Trans. Signal Process., vol. 42, no. 11, Nov. 1994:3084-91.
 - L. J. Yan and J. S. Pan, "Generalized discrete fractional Hadamard transformation and its application on the image encryption," in Proc. Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing, 2007:457–60.
 - N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Am. A 16, 1915 (1999).

- O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.* 24, 1999: 762-64.
- P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* 20, 1995:767-69.
- R. Tao, B. Deng, and Y. Wang, "Research progress of the fractional Fourier transform in signal processing," Springer, vol. 49, Jan 2006: 1-25.
- R. Tao, X. M. Li, and Y. Wang, "Generalization of the fractional Hilbert transform," *IEEE Signal Process. Lett.*, vol. 15, 2008:365-68.
- R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain," *Opt. Express*, vol. 15, no. 24, 2007:16067-69.
- S. C. Pei and M. H. Yeh, "Improved discrete fractional Fourier transform," *Opt. Lett.*, vol. 22, 1997:1047-49.
- S. C. Pei and W.L.Hsue, "Random discrete fractional Fourier transform," *IEEE Signal Process. Lett.*, vol. 16, no.12, Dec 2009:1015-18.
- S. C. Pei and W. L. Hsue, "The multiple-parameter discrete fractional Fourier transform," *IEEE Signal Process. Lett.*, vol. 13, no. 6, Jun. 2006:329-32.
- V. Namias, "The fractional order Fourier transform and its application to quantum mechanics," *J. Inst. Math. Appl.*, vol. 25, 1980:241-65.



Rajiv Saxena Dr. Saxena, born at Gwalior in Madhya Pradesh in 1961, obtained B.E. (Electronics & Telecommunication Engineering) in the year 1982 from Jabalpur University, Jabalpur. Subsequently, Dr. Saxena joined the Reliance Industries, Ahmedabad, as Graduate Trainee. In 1984, Dr. Saxena joined Madhav Institute of Technology & Science, Gwalior as Lecturer in Electronics Engineering. He obtained his M.E. (Digital Techniques & Data Processing) from Jiwaji University, Gwalior in 1990. The Ph. D. degree was conferred on him in 1996-97 in Electronics & Computer Engineering from IIT, Roorkee (erstwhile UOR, Roorkee). Currently Dr. Saxena is head and professor in ECE department at JUET, Guna.



Deepak Sharma completed his M. Tech. (Microwave Engineering) from Madhav Institute of Technology and Science in 2006. Before joining JUET, he worked as a Lecturer in Electronics Department, MITS, Gwalior (M.P). His Research areas include Antenna Theory, Radar System, Signal processing and Integral Transforms .